ELECTRONIC RECORDS MANAGEMENT GUIDELINES

E-MAIL MANAGEMENT

Summary

An electronic mail message or “e-mail” consists of a digitally stored message and any attached digital documents transferred between computer users. State and local governments use e-mail for a variety of tasks such as sending and receiving internal and external correspondence, distributing memos, circulating drafts, disseminating directives, transferring official documents, and supporting various business processes of the organization. Although few public agencies currently manage e-mail as records, both statute and case law make clear that e-mail must be included in your overall records management strategy.

E-mail documents that hold information about the day-to-day operation of state and local government must be easy to locate, those that hold information of long term or permanent value must be adequately protected, and those of transitory value must be deleted when no longer needed. Allowing e-mail to be managed by personal preference or routine systems back-ups and administrative procedures that treat all e-mail alike can result in serious legal, operational, and public relations risks. By establishing policies, applying records management procedures, and training users, you can create an environment that promotes successful management of e-mail records.

Legal Framework

For more information on the legal framework you must consider when managing e-mail, refer to *Records Management in an Electronic Environment* in the Electronic Records Management Guidelines and Appendix A6 of the *Trustworthy Information Systems Handbook*. Also review the requirements of the:

- South Carolina Public Records Act [PRA] (*Code of Laws of South Carolina, 1976*, Section 30-1-10 through 30-1-140, as amended) available at www.scstatehouse.org/code/t30c001.htm, which supports government accountability by mandating the use of retention schedules to manage records of South Carolina public entities. This law governs the management of all records created by agencies or entities supported in whole or in part by public funds in South Carolina. Section 30-1-70 establishes your responsibility to protect the records you create and to make them available for easy use. The act does not discriminate between media types. Therefore, records created or formatted electronically are covered under the act.
- South Carolina Uniform Electronic Transactions Act [UETA] (*Code of Laws of South Carolina, 1976*, Section 26-6-10 through 26-6-210), enacted in 2004, facilitates electronic commerce and electronic government services by legally placing electronic records and signatures on equal footing with their paper counterparts. UETA officially repeals the 1998 South Carolina Electronic Commerce Act (*Code of Laws of South Carolina, 1976*, Section 26-5-310 through 26-5-370). The purpose of UETA is to establish policy relating to the use of electronic communications and records in contractual transactions. This law does not require the use of electronic records and signatures but allows for them where agreed upon by all involved parties. While technology neutral, the law stipulates that all such records and signatures must remain trustworthy and accessible for later reference as required by law. Along a similar vein, the federal Electronic Signatures in Global and National Commerce (E-Sign) Act [U.S. Public Law 106-229] also encourages the use of electronic documents and signatures, although it goes further to provide some guidelines regarding standards and formats. For more information on UETA see Appendices A6 and A7 of the *Trustworthy Information Systems Handbook*.
- South Carolina Freedom of Information Act [FOIA] (*Code of Laws of South Carolina, 1976*, Section 30-4-10 through 30-4-165) supports government accountability by ensuring the right of citizens to inspect or copy public records. The establishment of fees, formal public notification, and restrictions limiting public disclosure of certain records is covered.

MORE →

Additional Legal Considerations

Within the context of these laws, you should also consider:

- *The ramifications of the Armstrong litigation*. In *Armstrong v. Executive Office of the President* (1 F.3d 1274 [DC Cir 1993]), a federal court found in favor of a group of researchers and nonprofit organizations who wanted to prevent the destruction of e-mail records created during the Reagan administration. The court determined that federal government agency e-mail messages, depending on content, are public records and that complete metadata must be captured and retained with the e-mail record. Although a federal decision, this litigation has strongly influenced government agencies at all levels. Other agencies are now paying closer attention to their e-mail records management practices, including the capture of metadata.
- *Legal discovery*. When developing your policy, balance your legal and operational requirements with the risk of being engaged in legal discovery. You must meet all government requirements for managing your e-mail records, but you should also be able to respond to discovery in an affordable, efficient, and practical way. Bear in mind that many courts have upheld discovery requests for e-mail records. For more information on the discovery of electronic records, refer to Appendix A7 of the *Trustworthy Information Systems Handbook*.
- The *Health Insurance Portability & Accountability Act of 1996* [HIPAA] (Public Law 104-191) which establishes security and privacy standards for health information. The Act protects the confidentiality and integrity of “individually identifiable health information,” past, present or future. Visit the South Carolina HIPAA website at www.hipaa.state.sc.us/ for additional information.

What is electronic mail?

E-mail is a confusing term because it can refer to both the system and the messages in the system. Furthermore, it can also be used to describe the action of sending or receiving a message. Here are some basic facts about e-mail to help clarify the process:

- E-mail is the exchange of computer stored information though a network. It relies on software applications and protocols (rules) to compose, transmit, receive, and manage e-mail messages.
- Users create and manage e-mail through e-mail accounts. Internet online services such as Yahoo and Google provide public accounts available to anyone. Private e-mail accounts, such as a work account, are limited to employees or individuals associated with an organization.
- Software applications, called e-mail clients, are used to compose, send, receive display and manage e-mail messages. The applications may be text or graphics based. Both proprietary and open source e-mail clients are available. They include Microsoft Outlook, Lotus Notes, Thunderbird, Pine, and Eudora. Internet sites such as MSN, Yahoo, and Google also provide e-mail capability using their software applications.
- Dedicated servers, known as e-mail servers, are often used to route and store large volumes of e-mail.
- Depending on your agency’s specific arrangement, e-mail servers can be housed internally in your agency and managed by your IT staff or housed and managed by others at a separate facility.
- Transactional information is information about an e-mail message. This metadata can include the name of the sender and all recipients, the date and time the message was created and sent. It may also include information on the systems and software applications used to create and transmit the message. Transactional information may not always be visible in every application but it is a vital part of every message and steps must be taken to preserve it.

Other electronic messaging systems

In addition to e-mail, there are other electronic messaging systems available to most organizations. Two popular systems are voice mail and instant messaging. A message created and managed in these systems may also be considered a record. Therefore, organizations should review all messaging systems in use and include any records covered under the existing records retention and disposition process. Work with your records management staff to develop new schedules where needed. For additional information on retention schedules, see the guideline *Records Management in an Electronic Environment*.

Voice mail

Voice mail is a highly sophisticated, computerized system for receiving, recording, saving, and managing voice messages. Although telephone-

MORE →

based voice mail is well-established in many organizations and used for important public business, it has rarely been managed as a record.

Recent technological advances that blur the distinction between e-mail and voice mail could make it easier to capture and manage audio records. New services including those utilizing Voice over Internet Protocol (VoIP) are capable of delivering messages as audio files via e-mail. Therefore, voice mail messages saved as e-mail can be managed along with other e-mail relating to the same topic.

Instant messaging

Instant messaging (IM) is a service that permits individuals to quickly exchange electronic messages with selected others in an informal manner that mimics conversation. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange that makes a continued exchange simpler than sending e-mail back and forth. Most exchanges are text-only, however, some services allow voice messaging and file sharing.

Designating e-mail as public records

Determining value and retention

The value of e-mail

Not all e-mail requires the same level of control. Although identification of e-mail records relating to the activities of public organizations will always be subjective, certain categories of records will typically be important to identify and manage. These include:

- Policies and directives
- Work schedules and assignments
- Drafts of documents circulated for approval or comment
- Any document that initiates, authorizes, or completes a business transaction
- Final reports or recommendations
- Correspondence, memos, or messages about agency or local government business
- Agendas and minutes of meetings

Declaring e-mail messages as records

Retention and disposition

Under the terms of the South Carolina Public Records Act, the South Carolina Department of Archives and History [SCDAH] administers South Carolina's program for the retention and disposition of public records. When thinking about e-mail records and retention schedules, it is important to remember that retention periods are based not on the method by which a record is created but rather on the legal, fiscal, administrative, or historical value of the information contained in the record. The application of record retention schedules does not change because a record is received or sent electronically.

Official copies

The official copy is the record copy — the document that constitutes the record of a business transaction.

Convenience copies

Convenience copies are duplicates of the record copy and have only temporary value. They can be disposed of at any time without authorization and should never be kept longer than the record copy.

Scheduling records

You must prepare record retention schedules in accordance with the Public Records Act to retain or dispose of all official copies of e-mail records relating to government business.

Other records

Transitory and personal messages that do not support government business as well as convenience or duplicate copies of e-mail records should be deleted from personal mailboxes when no longer needed. These include copies or extracts of documents distributed or received for reference — listserv or bulletin board posts, personal messages, announcements unrelated to official business, and announcements of social events like retirement parties or holiday celebrations. These materials consume disk space, erode the efficiency of the system, and, if kept, could be subject to freedom of information requests and discoverable in legal proceedings.

Retention periods

Generally, records transmitted through e-mail systems will have the same retention periods as records in other formats. E-mail letters and memos, for example, will be retained and disposed of according to the retention periods established for various types of correspondence. Many e-mail messages will be part of a distinct record series. Those messages should be retained and disposed of according to the retention period established for that series. You should use existing schedules to manage e-mail that has direct paper counterparts.

The SCDAH has issued several general record schedules for many types of records, common to state and local government, including

MORE →

correspondence. Records having no significance beyond their initial use should be destroyed, according to an approved retention schedule, when no longer needed for reference. Keep in mind that simply deleting a message may not remove it completely from the storage media. Utility programs are available to permanently remove electronic messages and eliminate the possibility of recovery.

Consult your records management staff or the SCDAH for advice on applying general record schedules.

Responsibility for retention

You must determine who is responsible for retention of the official copy. The chart below provides examples of the most common situations.

Who is Responsible for Maintaining E-mail?	
Message sent from outside the agency	**Message sent from inside the agency**
Retained by the person who receives e-mail	**Sender is responsible for maintaining if the message is complete and un-altered**
Exception: If the person receiving the message is not authorized to respond to the e-mail and forwards the message to someone else, the person receiving the forwarded message is responsible for maintaining it.	**Exception: If message is altered (responded to, edited, attachments added), the receiver is responsible for maintaining it. Keep in mind, if there are multiple replies between two or more people to the same message, only the final message needs to be saved PROVIDING that all of the replies are included in the final message.**

For additional information about retention and disposition, refer to the guideline, *Records Management in an Electronic Environment*.

Goals for successful e-mail management

Although your agency will develop unique procedures that meet your specific operational and legal requirements, bear in mind the following goals for an e-mail record. An e-mail record should be:

- *Complete*. E-mail records should completely document the transaction. For example, you cannot save the text without the sender information. Complete e-mail records must include all of the following elements, as applicable:
  - — Recipient(s)
  - — Sender
  - — Time sent
  - — Text
  - — Date sent
  - — Subject lines should clearly describe the contents of the message (e.g., the subject line "Correction" is inadequate. "Correction to Tourism Board Minutes 2005March15" provides a better description).
  - — Attachments should be included in full (not just indicated by file name).
  - — List members e-mailed using distribution lists. If an e-mail record simply lists the group name in the recipient field, the recipients must be identifiable. For example, the distribution list "HR" (a distribution list for all the members of the human resources department) should be documented so that each member of the list is named.
  - — Directory of e-mail addresses and the corresponding staff member names (e.g., jado25@myorg.net is Jane Doe). This connects an e-mail address listed in an e-mail record to a person.
- *Accurate*. The contents of the e-mail record should accurately reflect the transaction.
- *Accessible*. Some e-mail records must be accessible to the public and some should not depending on the content of the record and as determined by FOIA and HIPAA. All e-mail records, like other electronic records, should be reasonably accessible for the purposes of legal discovery.
- *Manageable*. E-mail records should be easy for staff members to manage as part of the daily workflow and records management practices. Because staff members will implement and use the e-mail records management policy, procedures should be straightforward.
- *Secure*. The e-mail record should reside in a secure system that controls access, storage, retrieval, alteration, and deletion. This is particularly important in controlling access to confidential e-mail records as determined by FOIA and HIPAA. E-mail records present unique

MORE →

security concerns, because e-mail messages are:

- Easily manipulated or deleted in the system
- Easily captured and read by unintended persons
- Easily forwarded and misdirected by mistake

Information technology departments rely on backup copies of data to replace information lost due to a catastrophic event. Although essential for disaster planning, backups are not an efficient or acceptable way to consistently manage important agency e-mail records. Adoption and oversight of an appropriate and secure recordkeeping system as described in this chapter and the *Trustworthy Recordkeeping Systems Handbook* is recommended.

Developing E-mail Policy

E-mail Policy Components

You should establish policies to guide users on questions of acceptable use, the management and retention of official copies, privacy, and access. All users should understand these policies and be able to apply them. The components of an e-mail retention policy should include information on:

Acceptable use

Written policies should be established for the use of e-mail in the same way they are established for the use of the telephone, fax machine, and postal mail.

Access

Because government e-mail can be defined as a public record, e-mail policies must comply with the state's Freedom of Information Act and Public Records Act. FOIA gives the public the right to access records, but it also limits access to some information considered personal or private. Custodians of public records must make their records available for public inspection provided that the information is not exempt from disclosure as determined by FOIA and HIPAA.

Privacy

Your policy should make it clear that although you attempt to provide security, e-mail messages sent or received are not private. They may be accessed and monitored by others, may be released to the public under provisions of FOIA, and may be subject to discovery proceedings in legal actions. Because computers can store messages at multiple locations within the system, even messages a user has deleted may be recoverable and used in a legal action.

Staff roles and responsibilities

Your policy should clearly define the roles and responsibilities that managers, network administrators, technical staff, records management staff, support staff, and users will have in the management of e-mail. It should clearly communicate whether the sender or the receiver should save e-mail records. The policy should guide staff members in determining which e-mail messages are records and outline a procedure for grouping e-mails into records series with a records retention schedule for each series.

Management and retention

Because the Public Records Act requires custodians to protect their records and to work with the SCDAH to establish retention periods, your policy should describe how and where you will maintain the official copies of your e-mail and provide for their management, protection, and retention for as long as they have administrative, legal, fiscal, or research value. For information on maintaining authentic and reliable records see the *Trustworthy Information Systems Handbook*.

Filing and maintenance

Only the official copy of those e-mail records that relate to agency or local government business functions need to be filed and maintained in a recordkeeping system. Additional copies, transitory communications, and personal messages can simply be deleted from the e-mail system when no longer needed. Include procedures for organizing, storing, maintaining, accessing, and disposing of e-mail records. Your policy should define how users are to manage their accounts including the regular removal of personal and transitory messages from their mail boxes.

Document Policy

Establish a procedure for documenting your e-mail records policy. On an on-going basis, from initial development onward, document the development of your e-mail records management policy, the policy itself, and changes to the policy. Include a description of the software and hardware in use, any training provided to staff, staff member responsibilities, and records retention schedules.

MORE →

Steps for better e-mail policy development

Use the following steps to guide you as you develop your e-mail records management policy:

1. Draft the policy and process with the input of stakeholders.
2. Allow stakeholders to review before finalizing the policy.
3. Implement the policy for staff members on a planned schedule and test the procedures.
4. Train the staff members on the new procedures. (Training is especially important because you must rely on staff members to ensure the integrity of the procedures.)
5. Document the policy.

Training for Staff Members

To ensure an effective system, you must provide user training and support. Your users should know how to identify the official copies of e-mail records. They should also know how to use the software to manage, protect, and provide access to the records. Your training and documentation should provide guidelines that staff members can follow to answer questions in the course of their work. Possible questions include:

- Is this e-mail an official record? Is this e-mail message administrative or personal (e.g., “Thursday staff meeting to start an hour late.” or “Let’s do lunch!”)?
- Does this e-mail message have long-term or permanent significance (e.g., “New policy finalized.”)? Does this e-mail message document a transaction or operations function (e.g., a process, a decision, or a discussion)?
- Is this e-mail record public or confidential as set forth by FOIA or HIPAA?
- What metadata must I capture when I save this e-mail record?
- To which records series does this e-mail record belong?
- Should I save the complete e-mail record, including attachments and group list names?
- Could this e-mail message be required as evidence in a legal action?

Preserving e-mail

You can use one of four methods to file and maintain your official copies of e-mail records:

- establish an electronic filing process
- maintain them in an electronic document management system
- print and file them in a manual system
- use a mix of manual and electronic systems and processes

Each method has its advantages and disadvantages; each requires a different degree of technical support; all require supervision and management. In making your selection, be sure that:

- it meets the needs of users
- it complies with all recordkeeping requirements.
- you have the tools, written policies and procedures
- users understand the policies and procedures, are familiar with the tools, and can apply all three consistently to all records

Option 1: Electronic filing

This method requires the establishment of an electronic filing process using a secure shared network server. The filing process should be used to collect and store related electronic records including, but not limited to, e-mail. A single employee or small group of employees should be appointed to oversee the process and system including the establishment of naming protocol and file structure. They should also be responsible for assigning access privileges to the system including delegation of privileges to add, delete or edit specific files and records. For suggestions on establishing naming conventions see the Electronic Records Management guideline *File Naming*.

Keep in mind that e-mail systems are not recordkeeping systems and messages should only be stored temporarily within an e-mail system. Retaining important e-mail within the e-mail system disconnects it from other related information and makes it susceptible to loss through regular system purges. If not immediately relocated to a separate electronic filing system, important messages should be removed from the e-mail client’s “inbox” and grouped into clearly named folders using the e-mail client software. Folders should later be exported to the electronic filing system.

Advantages. You retain the ability to easily search for, retrieve, or retransmit messages electronically. You may also retain important information related to the distribution of the e-mail. Depending on the filing arrangement used, it may be an effective way to integrate similar records that are created and received in electronic form.

MORE →

Disadvantages. The process requires active participation of all e-mail users. If not consistently and accurately managed, records are difficult to locate. Unless all records are in electronic format, you will also have to coordinate filing systems for records in both paper and electronic formats. Requires the use of a separate secure shared drive controlled by a limited number of employees to protect official copies from unauthorized access and prevent storage of duplicate copies.

Option 2: Electronic Document Management System

You can store, access, and manage e-mail messages and other electronic records in an Electronic Document Management System (EDMS).

Advantages. If the EDMS is secure and properly maintained, authorized users will enjoy consistently easy access to organizational records.

Disadvantages. Agencies must invest in an Electronic Document Management System [EDMS] that includes a records management application to support both operational and recordkeeping requirements. Unless all records are in electronic format, you will also have to coordinate filing systems for records in both paper and electronic formats. To maintain an electronic system for managing e-mail and other records, you must adopt standard practices to define documents, establish directories, and develop naming conventions for files. These standards are critical to access, retrieve, and share electronic records effectively. In addition, if you maintain records with lengthy retention periods solely in electronic systems, you will need to plan for the possibility of conversion and migration as hardware and software become obsolete. Technical and financial constraints may preclude some organizations from immediately investing in electronic recordkeeping for e-mail. However, you should consider an electronic solution when you update and redesign your systems. For more information on EDMSs, see the *Electronic Document Management Systems* guideline.

Option 3: Manual system

You can print your e-mail records and file the paper copies in a manual system.

Advantages. This method is easy to implement especially if you already have a well-designed filing system. It is also an effective way to integrate records that are created and received in both paper and electronic form.

Disadvantages. You lose the ability to easily search for, retrieve, or retransmit messages electronically if you print and then delete them. You may also lose important information related to the distribution of the e-mail. Furthermore, documents can be misfiled when users are responsible for printing, routing, and filing their own messages and this option consumes a great amount of paper and storage space. When choosing this method, you may want to print and file all information on addresses, recipients, distribution, transmission, and receipt of important e-mail documents.

Option 4: A mix of manual and electronic systems

Even when the goal is to install an electronic recordkeeping system for all records, most offices will have a transition period during which they will have to maintain records in both electronic and paper formats. When maintaining a mix of systems, you should make them as parallel as possible. Use similar file structures, naming conventions, and classifications for both systems, so the names of computer directories and subdirectories will mirror the names of your manual file cabinets, drawers, and folders.

Advantages. Records can be maintained in a way that best suits the existing recordkeeping environment and technological means of your organization.

Disadvantages. Most of the disadvantages of the other options are inherited. Multiple systems add extra complexity to implementation and can complicate records management. Furthermore, an indexing system is required to link the hardcopy and electronic materials.

Suggestions for better e-mail management

Policy

- ◆ Gather staff member input and support to ensure compliance with your e-mail management policy.
- ◆ Integrate your e-mail management policy with your overall electronic records management strategy. Review your policy and determine if you meet your legal and operational requirements.
- ◆ Determine ways to encourage staff member compliance so that policy is widely used and accepted, but causes minimal disruption to the daily operation.
- ◆ Determine the best way to train staff members. Decide how accountable staff members should be for compliance.

MORE →

Records Management

- ◆ Decide which e-mail messages are official records.
- ◆ Consider what elements of an e-mail record are needed for a complete understanding of the transaction.
- ◆ Determine the appropriate organization for long-term storage and access of e-mail records (e.g., project, department, function) and establish the appropriate records series and records retention schedules.
- ◆ Chose a storage medium to retrieve and dispose of e-mail.
- ◆ Decide how your e-mail retention strategy will coordinate with other records management procedures and systems (e.g., store all project-related e-mail with the other project documentation). Determine how records in other formats will be indexed.
- ◆ Determine the type and amount of documentation needed for the process.

Annotated List of Resources

Primary Resources

Ginn, M.L. *Guideline for Managing E-mail.* Prairie Village, KS: ARMA International, 2000.

Topics covered in this overview of e-mail management include organizational issues (e.g., legal, operational, governmental), creation and use of e-mail, and management of e-mail as a record (including filing, classification, backup, and disaster recovery).

South Carolina Department of Archives and History. *Trustworthy Information Systems Handbook*. Version 1, July 2004.
www.state.sc.us/scdah/erg/tis.htm

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

National Electronic Commerce Coordinating Committee. *Managing E-Mail.* December 2002.
www.ec3.org/Downloads/2002/managing_email.pdf

This guide tackles the perennial problem of e-mail management in a practical manner, offering model policies for use and retention, as well as a model user manual. While the policies acknowledge that e-mail is a record that should be managed on the basis of its content, the underlying assumption is that most e-mail has only transient value, and three retention periods (immediate destruction, limited retention, and archival retention) are proposed. A guide to implementing the models is also included.

Wallace, D.A. *Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice.* Proceedings of the Annual Meeting of the Society of American Archivists, September 3, 1998, Orlando, FL. Arlington, VA: Barry Associates; 1998:1-23.
www.mybestdocs.com/

This paper summarizes the issues surrounding e-mail policies and records management strategies. The paper describes e-mail records management policy elements and discusses the tasks and key concerns associated with the development of an e-mail records management policy.

Additional Resources

Utah State Archives and Records Services: Electronic Records
www.archives.state.ut.us/recmanag/electronic.htm

Visit this web site for links to the e-mail policies of a number of states in the United States, as well as links to additional web resources for records management.

Kentucky Department of Libraries and Archives. *Guidelines for Managing E-mail in Kentucky Government*
www.kdla.ky.gov/recmanagement/EmailGuidelines.pdf

Detailed guideline on the proper management of e-mail for government entities in Kentucky. Includes decision trees for determining e-mail retention and responsibility.